

UNITED STATES DISTRICT COURT

for the
Eastern District of North Carolina

FILED

SEP 12 2024

PETER A. MOORE, JR., CLERK
US DISTRICT COURT, EDNC
BY PS DEP CLK

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)64 GB SanDisk SD Card, PNY solid state drive model CS2140, Sea
Gate External Hard Drive (2TB), Predator Tritan 500 Laptop (Serial
number: NHQE8AA00114816D, located at Pender County Sheriff's
Office

Case No. 7:24-mj-1217-RJ

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
64 GB SanDisk SD Card, PNY solid state drive model CS2140, Sea Gate External Hard Drive (2TB), Predator Tritan 500 Laptop (Serial number: NHQE8AA00114816DE33400), located at Pender County Sheriff's Office, as described in attachment A.

located in the Eastern District of North Carolina, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, hereto and incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2252 and 2252A	Distribution, Receipt, and/or Possession Child Pornography
18 U.S.C. § 1466A	Distribution, Receipt and/or Possession of obscene material of a child

The application is based on these facts:
See attached affidavit which is attached hereto and incorporated herein by reference

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Addy Penniman
Applicant's signature

Addy Penniman, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: September 12 2024Robert B. Jones, Jr.
Judge's signatureCity and state: Wilmington, North Carolina

Robert B. Jones, Jr., United States Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR EASTERN DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH OF:
64 GB SanDisk SD Card
PNY solid state drive model CS2140
Sea Gate External Hard Drive (2TB)
Predator Tritan 500 Laptop (Serial number:
NHQE8AA00114816DE33400)

LOCATED AT:
Pender County Sheriff's Office
605 E. Fremont St. Burgaw, NC 28425

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Addy Penniman, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated electronic devices, more specifically described in the following paragraphs and in Attachment A.

2. I am a Special Agent ("SA") with the Department of Homeland Security (DHS) Homeland Security Investigations ("HSI") and have been since 2009. I am currently assigned to the HSI Office of the Resident Agent in Charge (RAC) Wilmington, North Carolina, which targets individuals involved in the sexual exploitation of children and other manners of commercial sex trafficking. As part of my duties and responsibilities, I investigate crimes involving the distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2252(a) and 2252A, and the distribution, receipt in obscene material of a child, in violation of 18 U.S.C. § 1466A. I have worked hundreds of cases involving child pornography, and executed or been on a team who has executed hundreds of search warrants. I have viewed millions of

images of child pornography and have a vast knowledge of investigating individuals who are involved in the sexual exploitation of children.

3. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the devices specifically described in Attachment A of this Affidavit, one (1) 64 GB SanDisk SD Card, one (1) PNY solid state drive model CS2140, one (1) Sea Gate External Hard Drive (2TB) and one (1) Predator Tritan 500 Laptop (Serial number: NHQE8AA00114816DE33400), (to be herein referred to as "SUBJECT DEVICES"). These SUBJECT DEVICES are believed to be accessed or used by Bryan Spencer INGRAM (Herein to be referred to as "SUBJECT PERSON"), for contraband and evidence, fruits, and instrumentalities of violations or attempted violations to distribution, receipt and possession of obscene material of a child, in violation of 18 U.S.C. § 1466A, and distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2252(a) and 2252A, which items are more specifically described in Attachment B of this Affidavit.

4. The statements contained in this affidavit are based in part on information provided by U.S. federal law enforcement agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents; information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by law enforcement agents/analysts and computer forensic professionals; and my experience, training and background as a Special Agent. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and

instrumentalities of violations or attempted violations of 18 U.S.C. § 1466A and 18 U.S.C. § 2252(a) and 2252A, are presently located in the SUBJECT DEVICES.

STATUTORY AUTHORITY

5. As noted above, this investigation concerns alleged violations of the following:

a. 18 U.S.C. § 1466A prohibits the distribution of a visual depiction of any kind, including a drawing, cartoon, sculpture, or painting, that depicts an image that is, or appears to be, of a minor engaging in graphic bestiality, sadistic or masochistic abuse, or sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, and lacks serious literary, artistic, political, or scientific value.

b. 18 U.S.C. § 2252(a) and 2252A prohibits a person from knowingly possessing or accessing sexually explicit images (child pornography) with the intent to view them as well as transporting, receiving, distributing or possessing in interstate or foreign commerce, or by using any facility or means of interstate or foreign commerce, any visual depiction of minors engaging in sexually explicit conduct (child pornography).

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachment B:

a. “Anime” as used herein, refers to refers to Japanese-style cartoon animation that is characterized by colorful graphics, vibrant characters, and fantastical themes, which may or may not include depictions of minors engaged in sexually explicit conduct.

b. “Computer-generated imagery (CGI), as used herein, refers to computer generated imagery created using computer software.

c. “Chat,” as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

d. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

e. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

f. “Cloud storage,” as used herein, is a form of digital data storage in which the digital data is stored on remote servers hosted by a third party (as opposed to, for example, on a user’s computer or other local storage device) and is made available to users over a network, typically the Internet.

g. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or

operating in conjunction with such device” and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

h. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, “thumb,” “jump,” or “flash” drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

i. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

j. “Computer-related documentation,” as used herein, consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

k. “Computer software,” as used herein, is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

l. A provider of “Electronic Communication Service” (“ESP”), as defined in 18 U.S.C. § 2510(15), is any service that provides to users thereof the ability to send or receive wire or electronic communications. For example, “telephone companies and electronic mail companies” generally act as providers of electronic communication services. See S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.

m. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

n. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

o. An “Internet Protocol address” or “IP address,” as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the

Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (“ISPs”) control a range of IP addresses. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

p. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

q. “Mobile applications,” as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

r. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

s. “Remote computing service,” as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

t. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation;

(d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

u. “Short Message Service” (“SMS”), as used herein, is a service used to send text messages to mobile phones. SMS is also often referred to as texting, sending text messages or text messaging. The service allows for short text messages to be sent from one cell phone to another cell phone or from the Web to another cell phone.

v. A “storage medium” is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, “thumb,” “jump,” or “flash” drives, CD-ROMs, and other magnetic or optical media.

w. “URL” is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

x. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

y. “Webcam,” as used herein, refers to a video camera that attaches to a computer or that is built into a laptop or desktop screen. It is widely used for video calling as well as to continuously monitor an activity and send it to a Web server for public or private viewing. Webcams generally have a microphone built into the unit or use the computer’s microphone for audio.

PROBABLE CAUSE

7. On July 11, 2024, the Pender County Sheriff's Office (PCSO), Detective Stephen Clinard received a call from Rachel Silver regarding a report filed with PCSO on June 29, 2024. Silver stated that she discovered a man, Bryan Spencer INGRAM (to herein be referred to as the SUBJECT PERSON), living/renting a room in her home, was a registered sex offender. She reported this information to a Deputy and learned there was a warrant for his arrest from the State of Washington. Silver reported meeting the SUBJECT PERSON while playing online games and offered to rent a room out of her house when he showed interested in moving to Pender County. Silver did not run a background check on the SUBJECT PERSON, and he paid her an entire year rent in advance. He moved into the residence in April 2024.

8. Silver stated while living together, the SUBJECT PERSON made inappropriate sexual comments about minors on television shows, additionally he would make comments about drinking urine, comments about feces and other inappropriate sexual remarks. Silver later started looking into the SUBJECT PERSON and found that he was a registered sex offender in the State of Washington.

9. Detective Clinard obtained a criminal history on the SUBJECT PERSON and found he was a registered sex offender and was currently listed with the Washington Department of Corrections as being wanted for an escapee from community custody for his convictions of possessing child pornography in 2018/2019. He is listed in their registry files as "non-compliant" and "moves without notification." Based on this information, Detective Clinard secured an arrest warrant for the SUBJECT PERSON.

10. On July 11, 2024, Detective Clinard approached the SUBJECT PERSON at his residence, 56 Henry Pridgen Drive, Burgaw, NC 28425 (herein to be referred to as, the

SUBJECT RESIDENCE), and placed him under arrest for failure to register as a sex offender, he was transported to the PCSO. The SUBJECT PERSON was advised of his Miranda rights, which he waived and agreed to speak with Det. Clinard.

11. During the interview of the SUBJECT PERSON, he admitted that he did not follow the law by failing to register as a sex offender in North Carolina. He admitted he was a registered sex offender and moved to North Carolina after erroneously researching the state and thinking he was free and clear from the duty to register. He admitted he had previously been charged and convicted of possessing child pornography but denied ever physically sexually abusing a "live" child. He claimed he was trying to lead a different life and was not looking at child pornography now. Det. Clinard asked for consent to search his cellular phone, the SUBJECT PERSON agreed and gave consent for Det. Clinard to look through his phone and perform a forensic extraction of his cellular phone.

12. On July 12, 2024, PCSO Det. Sgt. Brandenburg began the extraction of the SUBJECT PERSON's cellular phone. Det. Sgt. Brandenburg found multiple images depicting child pornography and/or obscene images in anime, cartoon, and artificial intelligence (AI) form. Many of these images depicted infant/toddler sexual abuse. Additionally, there were images of little girls faces that appear to have been obtained from the Discord Application (APP).

13. Det. Clinard applied for and was granted a state search warrant to enter the SUBJECT RESIDENCE, where he seized the SUBJECT DEVICES from the SUBJECT PERSON's bedroom.

14. Upon entering the room where the SUBJECT PERSON was residing at the SUBJECT RESIDENCE, Det. Clinard observed several bottles that appeared to be filled with

urine, feces stains in the seat of the chair and spattered on the wall in the closet, (where the SUBJECT PERSON was using as a computer gaming room), multiple pizza boxes and food and drink containers spread all over the room. Upon speaking with the roommate, Mrs. Silver, she stated the SUBJECT PERSON would spend days in his room without leaving. Det. Clinard seized SUBJECT DEVICES and transported them back to the PCSO.

15. On August 19, 2024, your affiant met with Det. Clinard to discuss this case. Your affiant reviewed the child pornography and/or obscene images depicted on the SUBJECT PERSON's cellular phone and describes a few of them as follows:

1. File name: barosu_036-847x751.jpg

Description: a color photo depicting a realistic image of an adult male, naked, holding his erect penis to the anus of an infant that is laying on the adults chest.

2. File name: drive1_8_020-847.jpg

Description: a color photograph depicting an adult male standing up naked with an erect penis.

The adult male is holding a naked prepubescent female, approximately 4-6 years old over his shoulder and using his fingers to pull apart her vagina. (This image is so realistic your affiant is not able to determine if it is CGI or real.)

3. File name: goldtod25_048-150x150.jpg

Description: a color photograph depicting an adult male penetrating the vagina of a female toddler with his erect penis. She is sucking her thumb and holding a stuffed animal.

4. File name: goldtod34_043-300x300.jpg

Description: color photograph depicting a female infant being gang raped by several adult males.

5. File name: ijp18_014-847x847.jpg

Description: a color photograph depicting an adult male who is naked from the waist down, who is penetrating the vagina of a female toddler in what appears to be a daycare setting.

16. Your affiant further reviewed the content extracted from the SUBJECT PERSONS phone and found over 250 images depicting child pornography and/or obscene images depicted in CGI/Anime form. Some of these images depicted child/infant rape scenarios. While some of the images were cartoon like, many of them were very realistic CGI-style, creating the need for a closer visual examination. During a key word search of the word “porn”, the web history of cellular phone showed links to “toddlercon-hentai”. Other terms searched by the SUBJECT PERSON, include, “teen only” and “underage”.

17. Based on the SUBJECT PERSON’s previous conviction for possession of child pornography, the SUBJECT PERSON’s clear evasion of law enforcement, failing to register as a sex offender in North Carolina, the large amount of images depicting child pornography and/or obscene images possessed in the SUBJECT PERSON’s cellular phone and the search terms he was using, your affiant believes that additional child pornography and/or obscene images will be found on the SUBJECT DEVICES.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

18. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as “WiFi” or “Bluetooth.” Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively, and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer’s ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types—to include computer hard drives, external hard drives, CDs, DVDs, and “thumb,” “jump,” or “flash” drives, which are very small devices that are plugged into a port on the computer—can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual’s person. Smartphones and/or mobile phones are also often carried on an individual’s person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography and/or obscene images in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography and/or obscene images. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as “cloud” storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography and/or obscene images can be found on the user’s computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as “apps.” Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography and/or obscene images, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography and/or obscene images may be stored.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one’s favorite websites in, for example, “bookmarked” files) or unintentional. Digital

information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO HAVE A SEXUAL
INTEREST IN CHILDREN OR WHO SOLICIT CHILD PORNOGRAPHY**

19. Based on my previous investigative experience related to child-exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who have a sexual interest in children and/or solicit child pornography and/or obscene images:

i. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

j. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

k. Such individuals almost always possess and maintain child pornographic material in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain those materials and child erotica for many years.

l. Likewise, such individuals often maintain their child pornography and/or obscene images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography and/or obscene images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography and/or obscene images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography and/or obscene images off their computers or digital devices on a cyclical and repetitive basis.

m. Importantly, evidence of such activity, including deleted child pornography and/or obscene images, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.¹

¹ See *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); see also *United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).

n. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain contact information (e.g., online messaging accounts, email addresses, etc.) of individuals with whom they have been in contact and who share the same interests in child pornography and/or obscene images.

o. Such individuals prefer not to be without their child pornography and/or obscene images for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

p. Even though an individual uses a portable device (such as the SUBJECT PHONE) to access the Internet to view child pornography and/or obscene images, it is more likely than not that evidence of this access will be found on the SUBJECT DEVICES as well, as set forth in Attachment A as well.

20. Based on all of the information contained herein, I believe that the SUBJECT PERSON likely displays characteristics common to individuals who have a sexual interest in children and/or solicits child pornography and/or obscene images.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

21. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT DEVICES, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

22. I submit there is probable cause to believe those records referenced above will be stored on the SUBJECT DEVICES, for at least the following reasons:

q. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

r. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

s. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

t. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

23. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the SUBJECT DEVICES were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the SUBJECT DEVICES.

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can

indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user’s state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner’s motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a “wiping” program to

destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography and/or obscene images, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for

evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

24. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to “cloud” storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search website all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain “booby traps” that destroy or alter data if certain procedures are not

scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

25. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of

wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

26. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

SEARCH METHODOLOGY TO BE EMPLOYED

27. The search procedure of electronic data contained in computer hardware, computer software, smartphone storage and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. on-site triage of computer systems (laptops, desktops, etc.) and/or mobile devices (smart phones, tablets, etc.) to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, as well as a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims;

b. examination of all of the data contained in such computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

c. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

d. surveying various file directories and the individual files they contain;

e. opening files in order to determine their contents;

f. scanning storage areas;

g. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and

h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

CONCLUSION

28. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits, and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the SUBJECT DEVICES described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

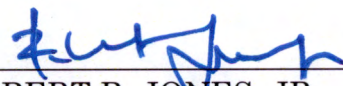
29. Because the warrant will be served on SUBJECT DEVICES that have already been seized, reasonable cause exists to support execution of the requested warrant at any time day or night.

30. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Addy Penniman

Addy Penniman
Special Agent
Homeland Security Investigations

On this 12 day of September 2024, Addy Penniman appeared before me via reliable electronic means, was placed under oath, and attested to the contents of this Affidavit.


ROBERT B. JONES, JR.
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

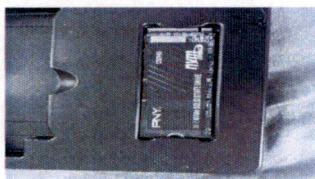
DESCRIPTION OF DEVICES TO BE SEARCHED

The following devices were seized by Pender County Sheriffs Office and are currently located at Pender County Sheriff's Office, 605 E. Fremont St. Burgaw, NC 28425, in their evidence room.

64 GB SanDisk SD Card



PNY solid state drive model CS2140



Sea Gate External Hard Drive (2TB)



Predator Tritan 500 Laptop (Serial number: NHQE8AA00114816DE33400)



ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. §§ 2252 and 1466A:

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which are stored records or information that is otherwise called for by this warrant (hereinafter, "SUBJECT DEVICES"
 - a. evidence of who used, owned, or controlled the SUBJECT DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the SUBJECT DEVICES, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;

- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;
 - e. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;
 - f. evidence of the attachment to the SUBJECT DEVICES of other storage devices or similar containers for electronic evidence;
 - g. evidence of programs (and associated data) that are designed to eliminate data from the SUBJECT DEVICES;
 - h. evidence of the times the SUBJECT DEVICES were used;
 - i. passwords, encryption keys, and other access devices that may be necessary to access the SUBJECT DEVICES;
 - j. documentation and manuals that may be necessary to access the SUBJECT DEVICES or to conduct a forensic examination of the SUBJECT DEVICES;
 - k. records of or information about Internet Protocol addresses used by the SUBJECT DEVICES;
 - l. records of or information about the SUBJECT DEVICES Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
 - m. contextual information necessary to understand the evidence described in this attachment.
3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography, as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2), to include cartoon, CGI, and child erotica.
5. Records, information, and items relating to violations of the statutes described above including:
 - a. Records, information, and items relating to the occupancy or ownership of the SUBJECT DEVICES including utility and telephone bills, mail envelopes, or addressed correspondence;
 - b. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;
 - c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;
 - d. Records and information relating to sexual exploitation of children, including correspondence and communications between users of child pornography and/or obscene material and exploitation websites and applications.
6. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to e-mail messages, chat logs, electronic messages, and other digital data files), pertaining to occupancy or ownership of the items to be searched described above, including, but not limited to, billing, account status, electronic receipts.

As used above, the terms “records” and “information” include all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing

or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro-SD cards, macro-SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.